REMARKS

In response to the Final Office Action, Claims 1, 20-22, 24 and 38-40 are amended. Claims 2, 6, 7, 27, and 28 were previously canceled. Claims 1, 3-5, 8-26 and 29-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

I. Objection to the Specification

The specification has been objected to as failing to provide proper antecedent basis for the claimed subject matter "the first random nonce N_B being unrelated to both K_B and S_B." However, the issue is moot in view of the above amendments.

II. Claims Rejected Under 35 U.S.C. §112

Claims 1, 3-5, 8-26 and 29-41 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement with respect to "the first random nonce N_B being unrelated to both K_B and S_B." However, the issue is moot in view of the above amendments.

III. Claims Rejected Under 35 U.S.C. §103

A. Claims 1, 3-5, 8-22, 24-26 and 29-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"), in view of Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, 1997, pages 234-237 ("Menezes") and further in view of *Simple Network Authenticating Key Exchange* ("SNAKE").

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Independent Claims 1, 20-22, 24 and 38-40 are amended to include the element of:

> "generating, at the first entity, a first secret S_B equal to a sequence of hash functions applied to at least a first password P_B, the first public key M_B, and the second public key M_A" (emphasis added).

Support for the amended limitation can be found, for example, in paragraphs 68 and 71 of the specification. Applicants submit that Vogelesang in view of Menezes and further in view of SNAKE does not teach or suggest the recited first secret S_B, which is equal to a sequence of hash functions applied to at least a first password P_B, the first public key M_B, and the second public key M_A.

Vogelesang discloses a cryptographic system in which signals between two participants are encrypted with one encryption key. The Examiner recognizes that Vogelesang does not disclose encryption with two encryption keys, but relies on Menezes to disclose double encryption, and SNAKE to disclose the generation of the first secret S_B. Based on the teaching of Menezes, the Examiner takes the position that the encryption key of Vogelesang can be combined with the encryption key of SNAKE, as the two recited keys K_B and S_B, to doubly encrypt a random number.

Applicants submit that SNAKE does not disclose the recited first secret S_B. SNAKE disclose a key exchange protocol in which a random number (S or R) is encrypted with a key K before transmission to another party (page 1). SNAKE discloses the key K for a Message3 is constructed as:

H(P, Message1, Message 2, $(g^{y[0]} \bmod f(0, P, R))^{x[0]} \bmod f(0, P, R)$, $(g^{y[1]} \bmod f(1, P, R))^{x[1]} \bmod f(1, P, R)$, ...), where H is a hash function and f is a function that constructs a large safe prime number.

SNAKE does not disclose the use of a sequence of hash functions. Rather, SNAKE only uses one hash function (H) in the construction of the key. The function f(0, P, R) is not a hash function, because it is used to generate prime numbers. Thus, SNAKE does not disclose the recited first secret S_B. The other cited references are not relied on for disclosing the first secret S_B. Thus, none of the cited references teach or suggest each of the elements of independent Claims 1, 20-22, 24 and 38-40, as well as their respective dependent claims.

Moreover, Applicants submit that the cited references cannot be combined to produce the claimed invention. The encryption key (S) of Vogelesang is used to encrypt a private message (e.g., a private signal D at col. 16, line 50-55), which is known only to the sender but unknown to the recipient. The encryption key (K) of SNAKE is used to encrypt a public message (e.g., S), which is known to both the sender and the recipient. In Response to Arguments, the Examiner

asserted that the encryption methods disclosed by the cited references can be performed on any type of message (Final Office Action on page 11). However, an encryption protocol, which includes multiple encryption operations, may be unable to protect an encrypted signal if the protocol does not comprise a proper sequence of operations performed on proper signals. An encryption protocol cannot be a secure protocol if it is formed by a patchwork of unrelated encryption operations. There is no teaching or suggestion in these references to combine an encryption key for a message known only to the sender with another encryption key for a message known to both the sender and the recipient. Thus, the proposed combination is inapposite.

Accordingly, reconsideration and withdrawal of the §103 rejection of Claims 1, 3-5, 8-22, 24-26 and 29-41 are respectfully requested.

B. Claim 23 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Vogelesang in view of Menezes and further in view of SNAKE.

Claim 23 depends from Claim 22 and incorporates the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 22, the cited references do not teach or suggest each of the elements of Claim 23.

Accordingly, reconsideration and withdrawal of the §103 rejection of Claim 23 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: October 30, 2007

Tong J. Lee, Reg. No. 48,582

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(310) 207-3800

CERTIFICATE OF ELECTRONIC FILING
I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below

Marilyn Bass October 30, 2007